Whitworth University urges patience after data breach, reported ransomware attack: 'This process does take time'

Greg Mason, Kip Hill

7-9 minutes

Whitworth University is taking steps to shore up its cyberdefenses following a reported ransomware attack that has left the university's network crippled since late last month.

Describing the incident as "a very sophisticated security issue involving our network systems," Whitworth officials said in a statement to the campus community that they first became aware July 29 that the university's information systems had been infiltrated by "outside actors."

It's unclear what sort of information may have been accessed as the investigation is ongoing.

If the investigation finds that any personal information of students, alumni, employees or donors was taken, Whitworth officials promised in a Wednesday letter to notify anyone affected right away and provide the necessary resources to protect their information.

"This process does take time," the letter reads. "Please know that your security and the protection of your personal information is of the utmost importance to us."

The university's technology and instructional resources teams have "worked tirelessly" alongside cybersecurity experts to stop the incident and restore systems as fast as possible, according to the letter. The school expects to have normal operations 95% restored by Aug. 31.

The university had been mum about what happened up until Wednesday, frustrating Whitworth students and parents just over a month ahead of the first day of fall classes on Sept. 7. University officials said they were comfortable releasing more details about the incidents now that a “final resolution” has been achieved.

Whitworth did not elaborate on the details of that resolution other than the school has added “new layers of systems protections” to better prevent future incidents, according to the statement.

Whitworth declined to comment further about the data breach, particularly in light of multiple reports that a group called LockBit is taking responsibility for the ransomware attack. Ransomware attacks encrypt data in demand of a ransom.

LockBit ransomware was first discovered three years ago and has become “the most prominent threat to several sectors” in 2022, said Nicole Hoffman, a senior cyberthreat intelligence analyst at the firm Digital Shadows, a London-based cybersecurity firm, in a statement.

In addition to stealing information, LockBit identifies its victims publicly online in an attempt to extort payment.

LockBit was blamed for a security breach at Accenture, an Irelandbased IT firm, in August 2021. LockBit demanded $50 million from the company, which refused to pay but later acknowledged some proprietary information was released.

Digital Shadows’ most recent report on ransomware activity, published July 11, found that LockBit was responsible for nearly one in three of all reported ransomware incidents posted on socalled “data leak” sites, where ransomware gangs demand payment for stolen data.

Roy Berg, whose son is an upperclassman, said he first noticed Whitworth’s issues upon trying to pay his son’s tuition July 28. He said he tried to call the university for a couple of days, but the phone lines wouldn’t go through, while the website was “completely dead.”

Berg’s son was able to confirm his fall schedule prior to the hack, though his Whitworth email was not working.

“All of my kid’s financial information, his Social Security number, his federal loan information – was that all hacked? We don’t know,” he said. “That’s what’s frustrating. What was it, and should we be signing up for identity protection?”

Upon finally managing to reach the university, Berg said Whitworth representatives declined to give him any additional information other than they were having “network difficulties.” While tuition was originally due Aug. 10, Berg said Whitworth did offer an indefinite extension on the deadline in light of the web issues.

Berg found out about the letter to the campus community through the media.

“Thanks, but it’s been nearly three weeks,” Berg said in response to the letter. “We’ve had no notification. We had nothing from anyone. Looking at it, it sounds like a press release.”

Mark Neufville, information and computer science instructor at Spokane Falls Community College, said institutions hit by ransomware often wait to notify the public.

“Usually when it happens, the thought process is you try to find out how big it is and how widespread it is before you start panicking the public,” he said. “Once that’s recognized and identified, then they go into this phase of, ‘Let’s try and stop it and solve it before it gets too big.’

“By then, you’re looking at a few weeks,” he continued. “Generally, they don’t like to put things out that they’re compromised until they actually put a solution in place.”

Panacea, not panic

Several provisions in Washington state law, some of them as recent as 2019, require entities that collect personal information to notify those whose information may have been taken in a security breach. However, the law provides an exemption “if the breach of the security of the system is not reasonably likely to subject consumers to a risk of harm.”

Such notification must be made within 30 days of the discovery of the breach, under Washington law. In addition, if more than 500 Washington residents must be notified, the entity must inform the Washington Attorney General’s Office.

That agency publishes a searchable database of businesses, government agencies and other entities that have had to inform their consumers that their data may have been stolen. The list includes at least one private higher education institution, including a notification in September 2020 that as many as 3,209

Washington residents at Notre Dame University, a private Catholic institution, may have been affected by a breach of the software company Blackbaud.

Blackbaud publicly admitted paying a ransom for stolen data to be deleted in that instance, drawing criticism from some security experts.

A report prepared by the Attorney General's Office in 2021 found that 6.3 million notices were sent to Washington residents about possible data breaches that year, an increase of nearly 500% over the year prior. The report found 150 malicious cyberattacks using ransomware in 2021, an increase from just seven such incidents in 2020.

"The biggest problem with data breaches is your hit to reputation," said Stu Steiner, assistant professor of computer science at Eastern Washington University. "A small company doesn't want to release too much information about it because they're going to take a huge reputation hit, and that could potentially put them out of business. I don't think that's going to happen in Whitworth's case."

In general, Steiner said any organization's first call with a ransomware attack is to the FBI. He said the FBI generally tells affected parties never to pay the ransom, as doing so could give more financial incentive to do more ransomware attacks.

Christian Parker, the supervisory senior agent for the FBI in Spokane, said on Tuesday he couldn't comment about the situation at Whitworth.

"Truthfully, most companies will end up probably paying because it's more expeditious than trying to reconstruct a month or two months' worth of data and get all of those records back," Steiner said. "It's probably a larger loss to not pay than it is to pay, but it's a tradeoff."

From there, Steiner said the affected organizations then typically connect with digital forensics professionals to determine when the systems were accessed, who did it, the timeframe, what data was affected and ways to restore the system back into compliance.

Reprinted from: https://www.spokesman.com/stories/2022/aug/18/whitworth-university-urges-patience-after-data-bre/